UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/605,644	10/15/2003	Steven L. Teixeira	VIV/0012.01	2643

28653 7590 12/12/2006

JOHN A. SMART
708 BLOSSOM HILL RD., #201
LOS GATOS, CA 95032

EXAMINER	
LASHLEY, LAUREL L	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/12/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/605,644	TEIXEIRA, STEVEN L.	
	Examiner	Art Unit	
	Laurel Lashley	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-55* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 55 are pending and have been examined.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 07/22/2004 was filed after the mailing date of the first Office action on the merits. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

3. Claims 1 –55 are rejected under 35 U.S.C. 102(e) as being anticipated by Margolus et al in US Patent Application Publication No. 2004/0162808 (hereinafter US PGPub '808).

As for claim 1, US PGPub '808 discloses:

In a computer system, a method for protecting sensitive information, the method comprising:

receiving input of sensitive information from a user;

computing a data shadow of the sensitive information for storage in a repository;

based on the data shadow stored in the repository, detecting any attempt to transmit the sensitive information; and

blocking any detected attempt to transmit the sensitive information that is not authorized by the user. (see Abstract; [0010] – [0012]; Figures 1 & 2)

For claim 2, US PGPub '808 discloses:

The method of claim 1, wherein said sensitive information comprises structured data. (see [0054], lines 3 – 9)

For claim 3, US PGPub '808 discloses:

The method of claim 2, wherein said data shadow is computed for the structured data as a regular expression and a hash. (see [0010], lines 4 – 9)

For claim 4, US PGPub '808 discloses:

The method of claim 3, wherein said hash comprises a MD-5 hash. (see [0059])

For claim 5, US PGPub '808 discloses:

The method of claim 2, wherein said structured data includes credit card number information. (see [0051], lines 4 –6; [0054], lines 3-9)

For claim 6, US PGPub '808 discloses:

The method of claim 2, wherein said structured data includes Social Security number information. (see [0051], lines 4 – 6; [0054], lines 3 – 9)

For claim 7, US PGPub '808 discloses:

The method of claim 3, wherein said regular expression represents formatting information for said structured data. (see 0054], lines 3 – 9)

For claim 8, US PGPub '808 discloses:

The method of claim 3, wherein said hash is computed after normalization of the structured data. (see [0054], lines 3 – 9)

For claim 9, US PGPub '808 discloses:

The method of claim 8, wherein said normalization includes removing any formatting information before computing the hash. (see [0059])

For claim 10, US PGPub '808 discloses:

The method of claim 1, wherein said sensitive information comprises structured data and said detecting step includes: initially detecting said structured data by matching a format for that structured data. (see [0054], lines 3 – 9)

For claim 11, US PGPub '808 discloses:

The method of claim 1, wherein said sensitive information comprises literal data. (see [0054], lines 3 – 9)

For claim 12, US PGPub '808 discloses:

The method of claim 11, wherein said data shadow is computed for the literal data as a length value plus at least one hash of the literal data. (see [0010], lines 4 – 9)

For claim 13, US PGPub '808 discloses:

The method of claim 12, wherein said at least one hash includes an additional first pass hash or checksum value computed for the literal data. (see Figure 5 & 6)

For claim 14, US PGPub '808 discloses:

The method of claim 12, wherein said at least one hash includes a MD-5 hash computed for the literal data. (see [0059])

For claim 15, US PGPub '808 discloses:

The method of claim 1, wherein said at least one hash includes an optional checksum value

computed for the literal data that allows relatively quick detection of the sensitive information and a MD-5 hash that allows subsequent verification. (see [0059]; [0066], lines 3 – 14)

For claim 16, US PGPub '808 discloses:

The method of claim 1, wherein said receiving input step includes: receiving input indicating a type for the sensitive information. (see [0054], lines 3 – 9)

For claim 17, US PGPub '808 discloses:

The method of claim 16, wherein said receiving input indicating a type includes: receiving input indicating that the sensitive information is a password. (see [0051])

For claim 18, US PGPub '808 discloses:

The method of claim 16, wherein said receiving input indicating a type includes: receiving input indicating that the sensitive information is a Social Security number. (see [0051])

For claim 19, US PGPub '808 discloses:

The method of claim 16, wherein said receiving input indicating a type includes: receiving input indicating that the sensitive information is a credit card number. (see [0051])

For claim 20, US PGPub '808 discloses:

The method of claim 16, wherein said receiving input indicating a type includes: receiving input indicating that the sensitive information is a personal identification number (PIN). (see [0051])

For claim 21, US PGPub '808 discloses:

The method of claim 1, further comprising: automatically determining a type for the sensitive information that indicates formatting. (see [0054]; [0062])

For claim 22, US PGPub '808 discloses:

The method of claim 21, wherein said step of automatically determining a type includes: matching the input against a template for identifying a type. (see [0051])

For claim 23, US PGPub '808 discloses:

The method of claim 1, wherein said detecting step includes: trapping an outbound buffer of data that may contain the sensitive information; and in instances where the sensitive information comprises structured data, performing a regular expression search on the outbound buffer. (see [0011]; [0064] - [0065]; Figure 5)

For claim 24, US PGPub '808 discloses:

The method of claim 23, further comprising: if a regular expression match is found, normalizing data from the match so as to remove formatting and thereafter computing a hash on it, for comparison with corresponding hash values stored in the repository. (see [0011])

For claim 25, US PGPub '808 discloses:

The method of claim 24, wherein said hash is a MD-5 hash. (see [0059])

For claim 26, US PGPub '808 discloses:

The method of claim 1, wherein said detecting step includes: trapping an outbound buffer of data that may contain the sensitive information; and in instances where the sensitive information comprises literal data, performing a sliding window search on the outbound buffer. (see Figure 5)

For claim 27, US PGPub '808 discloses:

The method of claim 26, wherein said sliding window search includes performing an optional checksum calculation on successive blocks of bytes within the outbound buffer, for comparison with corresponding checksum values stored in the repository. ([0011]; [0064]-[0065]; Figure 5)

For claim 28, US PGPub '808 discloses:

The method of claim 27, further comprising: if a match is found based on the checksum comparison, verifying the match with a MD-5 hash performed on data from the match. (see [0011]; [0048])

For claim 29, US PGPub '808 discloses:

The method of claim 28, wherein said MD-5 hash performed on data from the match is compared against a corresponding MD-5 hash value stored in the repository. (see [0011])

For claim 30, US PGPub '808 discloses:

The method of claim 1, wherein said step of blocking includes: referencing a stored policy indicating whether the sensitive information should be blocked from transmission. ([0012], lines 4-11)

For claim 31, US PGPub '808 discloses:

A computer-readable medium having processor-executable instructions for performing the method of claim 1. (see Abstract; Figures 1 – 10)

For claim 32, US PGPub '808 discloses:

A downloadable set of processor-executable instructions for performing the method of claim 1. (see Abstract; Figures 1 – 10)

As for claim 33, US PGPub '808 discloses:

In a computer system, a method for securing sensitive items from inappropriate access, the method comprising:

receiving input from a user indicating that a particular sensitive item is to be protected from inappropriate access;

storing metadata characterizing the particular sensitive item;

based on the stored metadata, detecting whether the particular sensitive item is present in any transmission of outgoing data; and

trapping any transmission of outgoing data that is detected to contain the particular sensitive item. (see Abstract; [0010] – [0012]; Figures 1 & 2)

For claim 34, US PGPub '808 discloses:

The method of claim 33, further comprising: a policy indicating what action the system should be taken upon trapping transmission of outgoing data that contains the particular sensitive item. (see [0011])

For claim 35, US PGPub '808 discloses:

The method of claim 34, wherein said action includes blocking any trapped transmission. (see [0012], lines 4 – 11)

For claim 36, US PGPub '808 discloses:

The method of claim 34, wherein said action includes querying the user about whether the particular sensitive item may be transmitted. (see [0011], [0012], lines 4 – 11; [0013])

For claim 37, US PGPub '808 discloses:

The method of claim 33, wherein said metadata includes a one-way hash of the particular sensitive item. (see [0059])

For claim 38, US PGPub '808 discloses:

The method of claim 37, wherein said one-way hash comprises a MD-5 hash. (see [0059])

For claim 39, US PGPub '808 discloses:

The method of claim 33, wherein said particular sensitive item comprises structured data, and wherein said metadata includes regular expression information characterizing a particular format for the structured data and includes a hash computed on unformatted data extracted from said structured data. (see [0059])

For claim 40, US PGPub '808 discloses:

The method of claim 39, wherein said trapping step includes: locating the particular sensitive item by first performing a regular expression search on the outgoing data for finding a match based on formatting; and for any match found based on formatting, performing a hash on the

match to determine whether it matches a corresponding hash stored as part of the metadata. (see [0059])

For claim 41, US PGPub '808 discloses:

The method of claim 33, wherein said particular sensitive item comprises literal data and wherein said metadata comprises as a length value plus at least one hash of the literal data. (see [0054], lines 3 - 9)

For claim 42, US PGPub '808 discloses:

The method of claim 41, wherein said trapping step includes: locating the particular sensitive item by first performing a sliding window search through the outgoing data for a block of bytes having a size equal to said length value and having a hash value equal to one of said at least one hash of the literal data. (see [0011]; [0064] – [0065]; Figure 5)

For claim 43, US PGPub '808 discloses:

The method of claim 42, wherein said at least one hash includes a MD-5 message digest computation. (see [0059])

For claim 44, US PGPub '808 discloses:

The method of claim 43, wherein said at least one hash further includes an optional first pass hash or checksum as an optimization. (see Figure 5 & 6)

For claim 45, US PGPub '808 discloses:

A computer-readable medium having processor-executable instructions for performing the method of claim 33. (see Abstract; Figures 1 – 10)

For claim 46, US PGPub '808 discloses:

A downloadable set of processor-executable instructions for performing the method of claim 33. (see Abstract; Figures 1 – 10)

As for claim 47, US PGPub '808 discloses:

A system providing security for sensitive information, the system comprising:

a data processing system receiving input of sensitive information;

a secure lockbox module for storing a secure descriptor characterizing the sensitive information; and a security module for detecting, based on said secure descriptor, any attempted transmission of outgoing data that contains the sensitive information. (see Abstract; [0010] – [0012]; Figures 1 & 2)

For claim 48, US PGPub '808 discloses:

The system of claim 47, wherein said input includes an indication of a type for the sensitive information. (see [0054], lines 3 –9)

For claim 49, US PGPub '808 discloses:

The system of claim 48, wherein said indication of a type includes a selected one of structured data and literal data. (see [0054], lines 3 – 9)

For claim 50, US PGPub '808 discloses:

The system of claim 49, wherein said structured data includes a credit card number. (see [0051])

For claim 51, US PGPub '808 discloses:

The system of claim 47, further comprising: a security policy specifying what action is to be undertaken when the security module detects an attempt to transmit the sensitive information. (see [0011]; [0012], lines 4 – 11)

For claim 52, US PGPub '808 discloses:

The system of claim 51, wherein said security policy specifies an action of blocking any attempted transmission of the sensitive information. (see [0011]; [0012], lines 4 – 11)

For claim 53, US PGPub '808 discloses:

The system of claim 51, wherein said security policy specifies an action of prompting a user to allow or deny any attempted transmission of the sensitive information. (see [0011]; [0012], lines 4 – 11)

For claim 54, US PGPub '808 discloses:

The system of claim 47, wherein said sensitive information includes structured data, and wherein said secure descriptor includes regular expression information characterizing a particular format for the structured data and includes a hash computed on unformatted data extracted from said structured data. (see [0054]; [0059])

For claim 55, US PGPub '808 discloses:

The system of claim 47, wherein said sensitive information includes literal data and wherein said secure descriptor includes a length value plus at least one hash of the literal data. (see [0054]; [0059])

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Rajasekaran et al. in US PGPub No. 2002/0174355 discloses techniques for searching encrypted files and Roginsky et al in US PGPub No. 2003/0084339 teaches hiding sensitive information.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurel Lashley whose telephone number is 571-272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Laurel Lashley
Examiner
Art Unit 2132

07 December 2006
LLL

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100